



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

5	<i>In re</i> Application of Goldberg, et al.  Serial No. 09/346,559  Filed: June 30, 1999  For: System For Authenticating Hardcopy Documents	) ) ) ) ) ) ) ) )	Group Art Unit: 2622  Examiner: Twyler M. Lamb
---	--	---	---

**APPEAL BRIEF**

15  
Box AF  
Assistant Commissioner for Patents  
Alexandria, VA 22313

**RECEIVED**

FEB 12 2004

Technology Center 2600

Sir:

20 **BRIEF ON BEHALF OF GOLDBERG, ET AL.:**

Appellant appeals from the Final Office action mailed on October 8, 2003, in which currently pending Claims 1-23 stand finally rejected. Appellant filed a Notice of Appeal via facsimile on December 5, 2003. This appeal brief is submitted in triplicate in support of Appellant's appeal.

**TABLE OF CONTENTS**

	1.	REAL PARTY IN INTEREST.....	3
	2.	RELATED APPEALS AND INTERFERENCES .....	3
	3.	STATUS OF CLAIMS.....	3
5	4.	STATUS OF AMENDMENTS.....	3
	5.	SUMMARY OF INVENTION .....	3
	6.	ISSUES.....	4
	7.	GROUPING OF CLAIMS .....	5
		A. Rejection Under 35 U.S.C. § 102(b).....	5
10		B. First Rejection Under 35 U.S.C. § 103(a).....	5
		C. Second Rejection Under 35 U.S.C. § 103(a).....	5
	8.	ARGUMENTS .....	6
		A. Rejection Under 35 U.S.C. § 102(b).....	6
		1. Grouping of Claims .....	6
15		2. '686 Reference (Zdybel).....	7
		4. Patentability of Group I Claims.....	8
		4. Patentability of Group II Claims .....	9
		5. Patentability of Group III Claims .....	10
		B. First Rejection Under 35 U.S.C. § 103(a).....	12
20		1. Grouping of Claims .....	12
		2. Patentability of Group I Claims.....	13
		3. Patentability of Group II Claims .....	13
		4. Patentability of Group III Claims .....	14
		C. Second Rejection Under 35 U.S.C. § 103(a).....	14
25		1. Patentability of Claims .....	14
	9.	CONCLUSION .....	15
	10.	APPENDIX .....	16

1. **REAL PARTY IN INTEREST**

The real party in interest is assignee Xerox Corporation, a New York Corporation, located at 800 Long Ridge Road, P.O. Box 1600, Stamford, CT 06904-1600.

5

2. **RELATED APPEALS AND INTERFERENCES**

There are no appeals or interferences known to Appellant, Appellant's legal counsel, or assignee, which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

10

3. **STATUS OF CLAIMS**

Finally-rejected claims 1-23 are pending and are the subject of this appeal. The claims involved in this appeal are included in the Appendix.

15 4. **STATUS OF AMENDMENTS**

A first non-final Office action ("first Office action") was mailed by the U.S. Patent & Trademark Office (USPTO) on January 29, 2003. In response, Appellant filed an Amendment Under 37 C.F.R. 1.116 ("first Response") on April 29, 2003. Claims 1 and 21-23 were amended. A Final Office action ("second Office action") was mailed by the USPTO on October 8, 2003. No Amendment After Final Office Action Pursuant to 37 C.F.R. § 1.116 was filed. A Notice of Appeal was filed via facsimile on December 5, 2003. Accordingly, no amendments have been filed subsequent to final rejection.

25 5. **SUMMARY OF INVENTION**

The invention provides a system and method for authenticating hardcopy documents by performing two independent operations: a signature generation operation and a signature verification operation (Spec. page 5, line 2-6; FIGS. 1, 5 and 6). Authentication allows a recipient to verify the integrity of digital data

using the public key of a sender by verifying a digital signature attached to the digital data, which was generated by the sender using a corresponding private key (Spec. page 1, lines 10-21). A scanned bitmap image of an original hardcopy document is recorded as grayscale image data or binary image data (Spec. page 6, lines 12-16). In one embodiment, the grayscale image data is compressed using a lossy compression scheme, including JPEG and wavelets, into compressed image data (Spec. page 6, line 24 through page 7, line 8). The compressed image data is used to produce an authentication token that represents a digital signature and the authentication token can be integrated with the grayscale image data to generate a signed hardcopy document, which can then be printed (Spec. page 7, lines 20-23). The authentication token includes a compressed representation of the original hardcopy document and means for authentication the document (Spec. page 7, lines 23-25). A private key of the sender, issued by a public-private key authority, is used to sign the original hardcopy document (Spec. page 7, lines 25-29). As a result, a recipient can authenticate, that is, verify the integrity of, the signed hardcopy document, by verifying the authentication token using the corresponding public key of the sender (Spec. page 11, lines 14-24).

## 6. ISSUES

There are three issues presented on appeal. First, whether claims 1, 7, 11-19, 21 and 23 are anticipated by U.S. Patent No. 5,486,686 (Zdybel, Jr. et al.) pursuant to 35 U.S.C. 102(b) (Issue I). Second, whether claims 2-5, 20 and 22 are obvious over Zdybel and further in view of U.S. Patent No. 5,157,726 (Merkle et al.) pursuant to 35 U.S.C. § 103(a) (Issue II). Third, whether claims 6 and 8-10 are obvious over Zdybel and further in view of U.S. Patent No. 5,706,099 (Curry) pursuant to 35 U.S.C. § 103(a) (Issue III).

**7. GROUPING OF CLAIMS**

**A. Rejection Under 35 U.S.C. § 102(b).**

Claims 1, 7, 11-19, 21 and 23 stand rejected under 35 U.S.C. § 102(b).

Appellant believes that the following groups of claims are separately patentable.

- 5 Claims 1, 7, 11-19, 21 and 23 do not stand or fall together, but instead are grouped together as follows:

Group I: Claims 1, 7 and 11-17

Group II: Claims 18 and 19

Group II: Claims 21 and 23

- 10 An argument in support of the foregoing groupings of claims 1, 7, 11-19, 21 and 23 is provided below in Section 8(A)(1).

**B. First Rejection Under 35 U.S.C. § 103(a).**

Claims 2-5, 20 and 22 stand rejected under 35 U.S.C. § 103(a). Appellant believes that the following groups of claims are separately patentable. Claims 2-

- 15 5, 20 and 22 do not stand or fall together, but instead are grouped together as follows:

Group I: Claims 2-5

Group II: Claim 20

Group II: Claim 22

- 20 An argument in support of the foregoing groupings of Claims 2-5, 20 and 22 is provided below in Section 8(B)(1).

**C. Second Rejection Under 35 U.S.C. § 103(a).**

Claims 6 and 8-10 stand rejected under 35 U.S.C. § 103(a) and stand or fall together.

8. ARGUMENTS

A. *Rejection Under 35 U.S.C. § 102(b).*

5 Claims 1, 7, 11-19, 21 and 23 stand rejected under 35 U.S.C. 102(b) as anticipated by Zdybel. A claim is anticipated under 35 U.S.C. 102(b) only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. MPEP § 2131. The Zdybel reference fails to teach each and every element of 1, 7, 11-19, 21 and 23. Applicant traverses the rejection.

1. Grouping of Claims

10 Group I consists of claims 1, 7 and 11-17, which define a method for authenticating a hardcopy document. Support can be found in the specification on page 6, line 13 through page 9, line 13. In particular, claim 1 recites arranging in a memory a scanned representation of a hardcopy document and a digital encoding of an authentication token for rendering a signed and authenticated  
15 hardcopy document. The authentication token is encoded using embedded digital data that is machine readable only. *See, e.g.,* Spec. page 8, lines 17-22. As claims 1, 7 and 11-17 recite a method with steps supportable by the specification distinctively from other apparatus and method claims, Group I properly states a separately patentable claim group.

20 Group II consists of claims 18 and 19, which define a method for authenticating a hardcopy document. Support can be found in the specification on page 13, line 14 through page 17, line 21. In particular, claim 18 recites arranging in a memory a digital encoding of authentication data for rendering a *label* containing a digital encoding of the authentication data. *See, e.g.,* Spec. page 15,  
25 line 21 through page 16, line 11 (“notary stamp 612”). In contrast, claim 1 renders a signed and authenticated *hardcopy document*. As claims 18 and 19 recite a method with steps supportable by the specification distinctively from other apparatus and method claims, Group II properly states a separately patentable claim group.

Group III consists of claims 21 and 23, which define a system for authenticating a scanned representation of a hardcopy document. Support can be found in the specification on page 5, line 3 through page 6, line 11. As claims 21 and 23 recite an apparatus with elements supportable by the specification  
5 distinctively from the other apparatus and method claims, Group III properly states a separately patentable claim group.

2. '686 Reference (Zdybel)

The Zdybel reference discloses hardcopy lossless data storage and electronic document processing, which tightly couples hardcopy output to  
10 electronic documents for enabling hardcopy documents to be employed as an essentially lossless medium (Abstract; Col. 4, lines 20-41). Documents are converted into electronic bitmap representations and converted into elemental textual and graphical encodings by employing recognition software (Col. 7, line 66-Col. 8, line 1). The electronic representation is composed of probabilistic  
15 encodings, bitmap images, or both (Col. 8, lines 23-29). Bit-level digital data contents of the electronic document are converted into "glyph encodings," which are encodings representing distinctive markings with at least two distinguishable, machine-readable states (Col. 8, lines 40-47). The glyph encodings can be used to recover data that affects the appearance of a document and data that is not  
20 inferable from the appearance of the document alone (Col. 9, lines 46-53). The glyph encoded data includes, by example, machine-readable descriptions of data points for structured graphics, algorithms utilized for performing computations for spreadsheets, hypertext pointer values, structural characteristics of the electronic source document, the document editor used to prepare the source document, the  
25 file name and storage location of the electronic source document, and an audit trail data for the electronic source document (Col. 10, lines 13-26). The glyph encodings are merged into an electronic document description file that causes the glyphs to be printed on the hardcopy output document (Col. 8, lines 47-50).

4. Patentability of Group I Claims

First, Claim 1 recites generating lossy compressed image data with the scanned representation of a hardcopy document. Support can be found in the specification on page 7, lines 11-19. In contrast, Zdybel discloses combining  
5 hardcopy output and electronic documents into a lossless communications medium (Abstract; Col. 4, lines 20-41) and not generating lossy compressed image data, per claim 1.

As well, Claim 1 recites producing an authentication token with the lossy compressed image data with the authentication token including encrypted image  
10 data or hashed encrypted image data. Support can be found in the specification on page 8, lines 1-16. In contrast, Zdybel discloses encoding bit-level digital data content into glyph encodings that can be used to recover data (Col. 8, lines 38-50). The glyph encodings represent the digital data content of ASCII, DDL or PDL encodings, which not equivalent to a public key corresponding to a private key of  
15 a sender. As a result, the glyph encodings do not form an authentication token and the integrity of the hardcopy output document generated by Zdybel cannot be verified by a recipient, per claim 1.

In fact, Zdybel teaches away from Claim 1 by describing the use of recognition software to extract semantic information in the form of bit-level  
20 digital data contents from a document (Col. 7, line 66-Col. 8, line 4). Zdybel creates the glyph encodings from the extracted semantic information (Col. 8, lines 41-48) and produces a machine readable digital representation and a human readable rendering on the same recording media using the same printing process (Col. 4, lines 45-51). In contrast, Claim 1 recites merely using the literal scanned  
25 representation of a hard copy document in the form of a lossy compressed image. Semantic information is not extracted. Further, Claim 1 defines authentication tokens produced using only the literal scanned representation and also recites generating lossy compressed image data, which is used to produce an authentication token that is arranged as a digital encoding with the scanned



representation for rendering at a printer. In summary, forming an authentication token is based only on the literal scanned representation in lossy compressed form and does not require recognition software, as disclosed in the Zdybel reference.

5 Claims 7 and 11-17 are dependent on Claim 1 and are patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. Accordingly, the Zdybel reference fails to described, either expressly or inherently, each and every claim element of Claims 1, 7 and 11-17. As Zdybel fails to anticipate Claims 1, 7 and 11-17, withdrawal of the rejection for anticipation is requested.

10 4. Patentability of Group II Claims

First, Claim 18 recites generating lossy compressed image data with the scanned representation of a hardcopy document. Support can be found in the specification on page 7, lines 11-19. In contrast, Zdybel discloses combining hardcopy output and electronic documents into a lossless communications  
15 medium (Abstract; Col. 4, lines 20-41) and not generating lossy compressed image data, per Claim 18.

As well, Claim 18 recites producing an authentication token with the lossy compressed image data with the authentication token including encrypted image data or hashed encrypted image data. Support can be found in the specification on  
20 page 8, lines 1-16. In contrast, Zdybel discloses encoding bit-level digital data content into glyph encodings that can be used to recover data (Col. 8, lines 38-50). The glyph encodings represent the digital data content of ASCII, DDL or PDL encodings, which not equivalent to a public key corresponding to a private key of a sender. As a result, the glyph encodings do not form an authentication token  
25 and the integrity of the hardcopy output document generated by Zdybel cannot be verified by a recipient, per Claim 18.

In fact, Zdybel teaches away from Claim 18 by describing the use of recognition software to extract semantic information in the form of bit-level digital data contents from a document (Col. 7, line 66-Col. 8, line 4). Zdybel

creates the glyph encodings from the extracted semantic information (Col. 8, lines 41-48) and produces a machine readable digital representation and a human readable rendering on the same recording media using the same printing process (Col. 4, lines 45-51). In contrast, Claim 18 recites merely using the literal  
5 scanned representation of a hard copy document in the form of a lossy compressed image. Semantic information is not extracted. Further, Claim 18 defines authentication tokens produced using only the literal scanned representation and also recites generating lossy compressed image data, which is used to produce an authentication token that is arranged as a digital encoding with the scanned  
10 representation for rendering at a printer. In summary, forming an authentication token is based only on the literal scanned representation in lossy compressed form and does not require recognition software, as disclosed in the Zdybel reference.

Claim 19 is dependent on Claim 18 and is patentable for the above-stated reasons, and as further distinguished by the limitations recited therein.  
15 Accordingly, the Zdybel reference fails to described, either expressly or inherently, each and every claim element of Claims 18 and 19. As Zdybel fails to anticipate Claims 18 and 19, withdrawal of the rejection for anticipation is requested.

#### 5. Patentability of Group III Claims

20 First, Claim 21 recites an image compression module generating lossy compressed image data with the scanned representation of a hardcopy document. Support can be found in the specification on page 7, lines 11-19. In contrast, Zdybel discloses combining hardcopy output and electronic documents into a lossless communications medium (Abstract; Col. 4, lines 20-41) and not  
25 generating lossy compressed image data, per Claim 21.

As well, Claim 21 recites an authentication token generator producing an authentication token with the lossy compressed image data with the authentication token including encrypted image data or hashed encrypted image data. Support can be found in the specification on page 8, lines 1-16. In contrast, Zdybel

discloses encoding bit-level digital data content into glyph encodings that can be used to recover data (Col. 8, lines 38-50). The glyph encodings represent the digital data content of ASCII, DDL or PDL encodings, which not equivalent to a public key corresponding to a private key of a sender. As a result, the glyph encodings do not form an authentication token and the integrity of the hardcopy output document generated by Zdybel cannot be verified by a recipient, per Claim 21.

In fact, Zdybel teaches away from Claim 21 by describing the use of recognition software to extract semantic information in the form of bit-level digital data contents from a document (Col. 7, line 66-Col. 8, line 4). Zdybel creates the glyph encodings from the extracted semantic information (Col. 8, lines 41-48) and produces a machine readable digital representation and a human readable rendering on the same recording media using the same printing process (Col. 4, lines 45-51). In contrast, Claim 21 recites merely using the literal scanned representation of a hard copy document in the form of a lossy compressed image. Semantic information is not extracted. Further, Claim 21 defines authentication tokens produced using only the literal scanned representation and also recites generating lossy compressed image data, which is used to produce an authentication token that is arranged as a digital encoding with the scanned representation for rendering at a printer. In summary, forming an authentication token is based only on the literal scanned representation in lossy compressed form and does not require recognition software, as disclosed in the Zdybel reference.

Claim 23 is dependent on Claim 21 and is patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. Accordingly, the Zdybel reference fails to described, either expressly or inherently, each and every claim element of Claims 21 and 23. As Zdybel fails to anticipate Claims 21 and 23, withdrawal of the rejection for anticipation is requested.

B. *First Rejection Under 35 U.S.C. § 103(a).*

Claims 2-5, 20 and 22 stand rejected under 35 U.S.C. § 103(a) as obvious over Zdybel and further in view of Merkle. To establish a *prima facie* case of obviousness: (1) there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or combine the reference teachings; (2) there must be a reasonable expectation of success; and (3) the combined references must teach or suggest all the claim limitations. MPEP § 2143. The combination of Zdybel and Merkle fail render Claims 2-5, 20 and 22 obvious. Applicant traverses the rejection.

1. Grouping of Claims

Group I consists of claims 2-5, which define a method for authenticating a hardcopy document. Support can be found in the specification on page 6, line 13 through page 9, line 13. In particular, claim 1, upon which claims 2-5 are dependent, recites arranging in a memory a scanned representation of a hardcopy document and a digital encoding of an authentication token for rendering a signed and authenticated hardcopy document. The authentication token is encoded using embedded digital data that is machine readable only. *See, e.g.*, Spec. page 8, lines 17-22. As claims 2-5 recite a method with steps supportable by the specification distinctively from other apparatus and method claims, Group I properly states a separately patentable claim group.

Group II consists of claim 20, which defines a method for authenticating a hardcopy document. Support can be found in the specification on page 13, line 14 through page 17, line 21. In particular, claim 18, upon which claim 20 is dependent, recites arranging in a memory a digital encoding of authentication data for rendering a *label* containing a digital encoding of the authentication data. *See, e.g.*, Spec. page 15, line 21 through page 16, line 11 (“notary stamp 612”). In contrast, claim 1 renders a signed and authenticated *hardcopy document*. As claim 20 recites a method with steps supportable by the specification distinctively

from other apparatus and method claims, Group II properly states a separately patentable claim group.

Group III consists of claim 22, which defines a system for authenticating a scanned representation of a hardcopy document. Support can be found in the specification on page 5, line 3 through page 6, line 11. As claim 22 recites an apparatus with elements supportable by the specification distinctively from the other apparatus and method claims, Group III properly states a separately patentable claim group.

## 2. Patentability of Group I Claims

As described above with reference to the rejection under 35 U.S.C. § 102(b) of Claims 1-7, 11-19, 21 and 23, the base reference, Zdybel, fails to teach or suggest all the claim elements. Thus, there would be no suggestion or motivation to modify the reference or combine the reference teachings nor would there be a reasonable expectation of success. Claims 2-5 are dependent on Claim 1 and are patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. Accordingly, the Zdybel and Merkle references, taken as a whole, fail to teach or suggest the claimed subject matter of claims 2-5. As Zdybel and Merkle fail to render claims 2-5 obvious, withdrawal of the rejection for obviousness is requested.

## 3. Patentability of Group II Claims

As described above with reference to the rejection under 35 U.S.C. § 102(b) of Claims 1-7, 11-19, 21 and 23, the base reference, Zdybel, fails to teach or suggest all the claim elements. Thus, there would be no suggestion or motivation to modify the reference or combine the reference teachings nor would there be a reasonable expectation of success. Claim 20 is dependent on Claim 18 and is patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. Accordingly, the Zdybel and Merkle references, taken as a whole, fail to teach or suggest the claimed subject matter of claim 20. As Zdybel and Merkle fail to render claim 20 obvious, withdrawal of the rejection for

obviousness is requested.

4. Patentability of Group III Claims

As described above with reference to the rejection under 35 U.S.C. § 102(b) of Claims 1-7, 11-19, 21 and 23, the base reference, Zdybel, fails to teach or suggest all the claim elements. Thus, there would be no suggestion or motivation to modify the reference or combine the reference teachings nor would there be a reasonable expectation of success. Claim 22 is dependent on Claim 21 and is patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. Accordingly, the Zdybel and Merkle references, taken as a whole, fail to teach or suggest the claimed subject matter of claim 22. As Zdybel and Merkle fail to render claim 22 obvious, withdrawal of the rejection for obviousness is requested.

C. *Second Rejection Under 35 U.S.C. § 103(a).*

Claims 6 and 8-10 stand rejected under 35 U.S.C. § 103(a) as obvious over Zdybel and further in view of Curry. Applicant traverses the rejection.

1. Patentability of Claims


As described above with reference to the rejection under 35 U.S.C. § 102(b) of Claims 1-7, 11-19, 21 and 23, the base reference, Zdybel, fails to teach or suggest all the claim elements. Thus, there would be no suggestion or motivation to modify the reference or combine the reference teachings nor would there be a reasonable expectation of success. Claims 6 and 8-10 are dependent on Claim 1 and are patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. Accordingly, the Zdybel and Merkle references, taken as a whole, fail to teach or suggest the claimed subject matter of claims 6 and 8-10. As Zdybel and Merkle fail to render claims 6 and 8-10 obvious, withdrawal of the rejection for obviousness is requested.

9. CONCLUSION

In view of the foregoing arguments, Applicant respectfully submits that the rejections under 35 U.S.C. § 102(b) and 35 U.S.C. §103(a) cannot be sustained and should be withdrawn. Reconsideration of the pending claims and a  
5 Notice of Allowance is respectfully solicited.

Please contact the undersigned at (206) 381-3900 regarding any questions or concerns associated with the present matter.

10 Dated: February 5, 2004

By:   
Patrick J.S. Inouye, Esq.  
Reg. No. 40,297

15 Law Offices of Patrick J.S. Inouye  
810 Third Avenue  
Suite 258  
Seattle, WA 98199

Telephone: (206) 381-3900  
Facsimile: (206) 381-3999

20 Appeal Brief

**10. APPENDIX**

1           1.       (Previously amended) A method for authenticating a hardcopy  
2 document, comprising the steps of:  
3           recording in a memory a scanned representation of the hardcopy document  
4 at a selected resolution;  
5           generating lossy compressed image data with the scanned representation of  
6 the hardcopy document;  
7           producing an authentication token with the lossy compressed image data;  
8 the authentication token including one of encrypted image data and hashed  
9 encrypted image data; the hashed encrypted image data including the lossy  
10 compressed image data and an encrypted hash of the lossy compressed image  
11 data; and  
12           arranging in the memory the scanned representation of the hardcopy  
13 document with a digital encoding of the authentication token for rendering at a  
14 printer a signed and authenticated hardcopy document.

1           2.       (Original) The method according to claim 1, further comprising the  
2 step of verifying the signed hardcopy document by:  
3           recording a scanned representation of the signed hardcopy document;  
4           decoding the authentication token from the scanned representation of the  
5 signed hardcopy document;  
6           authenticating the lossy compressed image data using one of the encrypted  
7 image data and the hashed encrypted image data; and  
8           decompressing the authenticated lossy compressed image data for  
9 comparison with the signed hardcopy document to determine whether the signed  
10 hardcopy document is authentic.

1           3.       (Original) The method according to claim 2, further comprising the  
2 step of visually comparing the signed hardcopy document with the authenticated  
3 lossy compressed image data.



1           4.       (Original) The method according to claim 2, further comprising the  
2 step of visually comparing the signed hardcopy document with a printed hardcopy  
3 document of the authenticated lossy compressed image data.

1           5.       (Original) The method according to claim 2, wherein said step of  
2 producing an authentication token is performed with a private key and said step of  
3 authenticating lossy compressed image data is performed with a public key.

1           6.       (Original) The method according to claim 1, further comprising the  
2 step of encoding the authentication token in a low intensity background pattern.

1           7.       (Original) The method according to claim 1, further comprising the  
2 step of encoding the authentication token in embedded data.

1           8.       (Original) The method according to claim 7, wherein said encoding  
2 step encodes the authentication token in a halftone pattern.

1           9.       (Original) The method according to claim 8, wherein said encoding  
2 step encodes the authentication token in a hyperbolic halftone pattern.

1           10.      (Original) The method according to claim 8, wherein said encoding  
2 step encodes the authentication token in a serpentine halftone pattern.

1           11.      (Original) The method according to claim 7, wherein said encoding  
2 step encodes the authentication token in data glyphs.

1           12.      (Original) The method according to claim 1, wherein said step of  
2 generating lossy compressed image data loses document formatting contained in  
3 the scanned representation of the hardcopy document.

1           13.      (Original) The method according to claim 12, wherein said step of  
2 generating lossy compressed image data further comprises the step of compressing  
3 the scanned representation of the hardcopy document by identifying exemplars

4 and locations of exemplars; each exemplar identified representing one or more  
5 image segments from the scanned representation of the hardcopy document.

1 14. (Original) The method according to claim 13, wherein said  
2 compressing step records the exemplars at a resolution that is less than the  
3 selected resolution of the scanned representation of the hardcopy document.

1 15. (Original) The method according to claim 13, wherein said  
2 compressing step records that locations of exemplars at a resolution that is less  
3 than the selected resolution of the scanned representation of the hardcopy  
4 document.

1 16. (Original) The method according to claim 1, wherein said  
2 compressing step compresses identified portions of the image data at a plurality of  
3 compression ratios.

1 17. (Original) The method according to claim 16, further comprising  
2 the step of segmenting text data from pictorial data before compressing the  
3 scanned representation of the hardcopy document.

1 18. (Original) A method for authenticating a hardcopy document,  
2 comprising the steps of:  
3 recording in a memory a scanned representation of the hardcopy document  
4 at a selected resolution;  
5 generating lossy compressed image data with the scanned representation of  
6 the hardcopy document;  
7 producing an authentication token with the lossy compressed image data;  
8 the authentication token including one of encrypted image data and hashed  
9 encrypted image data; the hashed encrypted image data including the lossy  
10 compressed image data and an encrypted hash of the lossy compressed image  
11 data; and

12           arranging in the memory a digital encoding of the authentication data for  
13 rendering at a printer a label containing the digital encoding of the authentication  
14 data.

1           19.   (Original) The method according to claim 18, further comprising  
2 the step of fixedly attaching the label to the hardcopy document to produce a  
3 signed hardcopy document.

1           20.   (Original) The method according to claim 19, further comprising  
2 the step of verifying the signed hardcopy document by:  
3           recording a scanned representation of the signed hardcopy document;  
4           decoding the authentication token from the scanned representation of the  
5 signed hardcopy document;  
6           authenticating the lossy compressed image data using one of the encrypted  
7 image data and the hashed encrypted image data; and  
8           decompressing the authenticated lossy compressed image data for  
9 comparison with the signed hardcopy document to determine whether the signed  
10 hardcopy document is authentic.

1           21.   (Previously amended) A system for authenticating a scanned  
2 representation of a hardcopy document, comprising:  
3           an image compression module for generating lossy compressed image data  
4 with the scanned representation of the hardcopy document;  
5           an authentication token generator for producing an authentication token  
6 with the lossy compressed image data; the authentication token including one of  
7 encrypted image data and hashed encrypted image data; the hashed encrypted  
8 image data including the lossy compressed image data and an encrypted hash of  
9 the lossy compressed image data; and  
10          an encoding module for arranging the scanned representation of the  
11 hardcopy document with a digital encoding of the authentication token for  
12 rendering at a printer a signed and authenticated hardcopy document.

1           22.   (Previously amended) The system according to Claim 21, further  
2 comprising:  
3           a memory for recording the signed hardcopy document;  
4           a decoding module for decoding the signed hardcopy document to define  
5 decoded signed image data;  
6           an authentication module to authenticating the decided signed image data  
7 using of the encrypted image data and the hashed encrypted image data to define  
8 authenticated image data; and  
9           a decompression module for decompressing the authenticated image data  
10 to define decompressed image data;  
11           means for comparing the signed hardcopy document with the authenticated  
12 hardcopy document to determine whether the signed hardcopy document is  
13 authentic.

1           23.   (Previously amended) The system according to Claim 21, wherein  
2 said image compression module compresses the scanned representation of the  
3 hardcopy document by identifying exemplars and locations of exemplars; each  
4 exemplar identified representing one or more image segments from the scanned  
5 representation of the hardcopy document.

1